

(12/31/1995)

ALL FBI INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-17-2012 BY 60324/UC/baw/sab/aio

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Precedence: PRIORITY

Date: 02/12/1998

To: All Field Offices

Attn: CITA Supervisors

From: NSD/CID
CITAC/Room 11887
Contact: SSA [redacted]

Approved By: [redacted] JPO/kj
Geide Kenneth M [redacted]
[redacted] [initials]

b6
b7C

Drafted By: [redacted] daf

Case ID # (U) ~~(S)~~ 288-HQ-1242560-⁵² (Pending)

Title: (U) ~~(S)~~ CHANGED TITLE
SOLAR SUNRISE;
CITA MATTERS;
OO: HQ;

Synopsis: (U) To provide a synopsis of investigative matter and set-forth leads for each Field Office.

(U) ~~(S)~~

Classified By: 4511, CITAC/D5
Reason : 1.5(c)
Declassify On: 2/12/2008

Administrative: (U) ~~(S)~~ Reference Bureau teletype, dated 2/6/1998, to all field offices captioned "COMPUTER INTRUSIONS," 288-HQ-A1220460, and Bureau EC to all field offices, dated 2/9/1998, captioned "UNSUB(S); MULTIPLE INTRUSIONS INTO DOD NETWORKS; CITA MATTERS; OO: HQ."

Details: (U) ~~(S)~~ By way of background, on February 1, 1998, DOD began detecting computer intrusions into its unclassified computer systems at various facilities in the United States (U.S.). These intrusions are ongoing. At least 11 DOD systems are known to have been compromised and recovery procedures have

~~SECRET~~

uploaded 2/15/98

[redacted], Am731

b6
b7C

~~SECRET~~

To: All Field Offices From: NSD/CID
Re (U) ~~(S)~~ 288-HQ-1242560, 02/12/1998

been initiated. The intruder appears to have targeted domain name servers and obtained root status via exploitation of the "statd" vulnerability in the Solaris 2.4 operating system. Hacker tools imported from a University of Maryland site were used to gain entry. The intruder installed a sniffer program and then closed the vulnerability by transferring a patch from the University of North Carolina. A "backdoor" was created to, allow the intruder reentry to the system.

Referral/Consult

(U) ~~(S)~~ Numerous university computer sites in the U.S. appear to have been exploited in similar fashion. Internet service providers near those universities also appear to have been exploited to access, or attempt to access, DOD computer networks.

Referral/Consult

Referral/Consult

~~SECRET~~

~~SECRET~~

To: All Field Offices From: NSD/CID
Re:(U) ~~(S)~~ 288-HQ-1242560, 02/12/1998

(U) The following leads are being set forth.

~~SECRET~~

~~SECRET~~

To: All Field Offices From: NSD/CID
Re: (U) (S) 288-HQ-1242560, 02/12/1998

LEAD (s):

Set Lead 1:

ALL RECEIVING OFFICES

(U) (S) 1. Will expeditiously contact all logical sources for any information pertaining to intrusions into Air Force domain name servers using the "statd" exploit on Solaris 2.4 operating system. Will respond expeditiously with positive results to SSA [redacted] or SSA [redacted] telephone [redacted]

b6
b7C

Set Lead 2:

WASHINGTON FIELD OFFICE, NVRA

(U) (S) 1. Will conduct appropriate investigation at the University of Maryland to determine source of hacker tools associated with Air Force DNS intrusions. Contact should be made with [redacted] University of Maryland, [redacted] WFO will obtain all necessary orders from DOJ to gain access to files and log data.

Referral/Consult

b6
b7C

(U) (S) [redacted]
[redacted] Thereafter, conduct appropriate follow up investigation.

(U) (S) 3. WFO National Computer Crimes Squad will open a separate investigation into [redacted]
[redacted] date of birth [redacted] focusing on intrusions occurring at U.S. Naval bases. Will establish contacts and coordinate investigation with NCIS.

b6
b7C

~~SECRET~~

~~SECRET~~

To: All Field Offices From: NSD/CID
Re:(U) ~~(S)~~ 288-HQ-1242560, 02/12/1998

CC: 1 - [redacted]
1 - Mr. Geide
1 - [redacted]
1 - [redacted]

b6
b7C

♦♦

~~SECRET~~